submitting person or entity, or is otherwise not appropriate for such disclosure.

(k) *Obtaining written consent for further disclosure from the person or entity submitting information.* (1) Authority to Seek and Obtain Submitter's Consent to Disclosure. The Protected CII Program Manager or any Protected CII Program Manager's designee may seek and obtain written consent from persons or entities submitting information when such consent is required under the CII Act of 2002 to permit disclosure. In exigent circumstances, and so long as contemporaneous notice is provided to the Protected CII Program Manager or the Protected CII Program Manager's designees, any Federal government employee may seek the consent of the submitting party to the disclosure of Protected CII where such consent is required under the CII Act of 2002.

(2) Consequence of Consent. Whether given in response to a request from the Protected CII Program Manager, the Protected CII Program Manager's designees, or another Federal government employee pursuant to paragraph (k)(1) of this section, a person's or entity's consent to additional disclosure, if conditioned on a limited release of Protected CII that is made for DHS's purposes and in a manner that offers reasonable protection against disclosure to the general public, shall not result in the information's loss of treatment as Protected CII.

§ 29.9 Investigation and reporting of violation of protected CII procedures.

(a) *Reporting of possible violations.* Persons authorized to have access to Protected CII shall report any possible violation of security procedures, the loss or misplacement of Protected CII, and any unauthorized disclosure of Protected CII immediately to the Protected CII Program Manager or the Protected CII Program Manager's designees who shall in turn report the incident to the IAIP Directorate Security Officer and to the DHS Inspector General.

(b) *Review and investigation of written report.* The Inspector General, Protected CII Program Manager, or IAIP Security Officer shall investigate the incident and, in consultation with the DHS Office of the General Counsel, determine whether a violation of procedures, loss of information, and/or unauthorized disclosure has occurred. If the investigation reveals any evidence of wrongdoing, DHS, through its Office of the General Counsel, shall immediately contact the Department of Justice's Criminal Division for consideration of prosecution under the criminal penalty provisions of section 214(f) of the CII Act of 2002.

(c) *Notification to originator of Protected CII.* If the Protected CII Program Manager or the IAIP Security Officer determines that a loss of information or an unauthorized disclosure has occurred, the Protected CII Program Manager or the Protected CII Program Manager's designees shall notify the submitter of the information in writing, unless providing such notification could reasonably be expected to harm the investigation of that loss or any other law enforcement, national security, or homeland security interest. The written notice shall contain a description of the incident and the date of disclosure, if known.

(d) *Criminal and administrative penalties.* As established in section 214(f) of the CII Act, whoever, being an officer or employee of the United States or of any department or agency thereof, knowingly publishes, divulges, discloses, or makes known in any manner or to any extent not authorized by law any information protected from disclosure by the CII Act of 2002 and coming to the officer or employee in the course of his or her employment or official duties or by reason of any examination or investigation made by, or return, report, or record made to or filed with, such department or agency or officer or employee thereof, shall be fined under title 18 of the United States Code, imprisoned not more than one year, or both, and shall be removed from office or employment.